

AMENDMENTS TO THE CLAIMS:

Please amend the claims as follows:

Claims 1-7. (cancelled)

8.(currently amended): A network system providing secure communication services, comprising:

a plurality of pieces of switching equipment, being connected to each other through a public network, and accommodating data terminals; and

central management and control equipment connected to the plurality of pieces of switching equipment through a separate network different from the public network,

wherein the central management and control equipment includes a database storing a plurality of sets of a public key and a private key, each assigned to a piece of switching equipment,

a first piece of switching equipment, accommodating a data terminal of a calling party, [[transmits]] encrypts a dial number of a called party and a user number of the first piece of switching equipment by using a public key, which is used between the first piece of switching equipment and the central management and control equipment and transmits the encrypted dial number and user number to the central management and control equipment via the separate network,

the central management and control equipment decrypts the transmitted dial number and user number, retrieves a public key of a second piece of switching equipment accommodating a data terminal of the called party corresponding to the decrypted dial number and a common key, which is used between the first and second pieces of switching equipment,

[[sends]] encrypts the retrieved public key of the second piece of switching equipment and the common key, which is used between the first and second pieces of switching equipment by using a public key of the first piece of switching equipment, and second the encrypted public key and common key to the first piece of switching equipment via the separate network,

the first piece of switching equipment [[encrypts]] decrypts the public key and common key sent from the central management and control equipment, encrypts the decrypted common key, which is used between the first and second pieces of switching equipment by using the public key of the second piece of switching equipment and sends the encrypted common key by the public key of the second piece of switching equipment to the second piece of switching equipment via the public network, and

the second piece of switching equipment decrypts the encrypted common key sent from the first piece of switching equipment by a private key of the second piece of switching equipment, so that the common key can be used to perform secure communication between the first and second pieces of switching equipment.

9.(currently amended): The network system providing secure communication services according to claim 8 [[1]],

wherein the separate network is central management and control equipment is connected to the plurality of pieces of switching equipment by a No. 7 common channel signaling network, and the first piece of switching equipment encrypts the dial number of the called party and the user number of the first piece of switching equipment by using a common key used between the first piece of switching equipment and the central management and control equipment when transmitting them to the central management and control equipment.

10.(currently amended): The method for providing secure communication services
~~network system providing secure communication services~~ according to claim 12 [[1]],

wherein the separate network is a No. 7 common channel signaling network
~~central management and control equipment encrypts the public key of the second switching
equipment and the common key used between the first and second pieces of switching equipment
to transmit them to the first piece of switching equipment, and the first piece of switching
equipment decrypts the common key used between the first and second pieces of switching
equipment by a private key to the first piece of switching equipment.~~

11.(canceled):

12.(currently amended): A method for providing secure communication services in a
network system having a plurality of pieces of switching equipment, being connected to each
other through a public network, and accommodating data terminals, and central management and
control equipment connected to the plurality of pieces of switching equipment through a separate
network different from the public network, the method comprising the steps of:

in a database provided at the central management and control equipment, storing a
plurality of sets of a public key and a private key, each assigned to a piece of switching
equipment;

from a first piece of switching equipment accommodating a data terminal of a
calling party, [[transmitting]] encrypting a dial number of a called party and a user number of the
first piece of switching equipment by using a public key, which is used between the first piece of

switching equipment and the central management and control equipment, and transmitting the encrypted dial number and user number to the central management and control equipment via the separate network;

in the central management and control equipment, decrypting the transmitted dial number and user number, retrieving a public key of a second piece of switching equipment accommodating a data terminal of the called party corresponding to the decrypted dial number and a common key, which is used between the first and second pieces of switching equipment, [[sends]] encrypting the retrieved public key of the second piece of switching equipment and the common key, which is used between the first and second pieces of switching equipment by using a public key of the first piece of switching equipment, and sending the encrypted public key and common key to the first piece of switching equipment;

by the first piece of switching equipment, [[encrypting]] decrypting the public key and common key sent from the central management and control equipment, encrypting the decrypted common key, which is used between the first and second pieces of switching equipment by using the public key of the second piece of switching equipment, and sending the encrypted common key by the public key of the second piece of switching equipment to the second piece of switching equipment via the public network; and

by the second piece of switching equipment, decrypting the encrypted common key sent from the first piece of switching equipment by a private key of the second piece of switching equipment, so that the common key can be used to perform secure communication between the first and second pieces of switching equipment.